UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,490	12/31/2003	Priya Govindarajan	110466-152114	1801

31817 7590 06/29/2007

SCHWABE, WILLIAMSON & WYATT, P.C.
PACWEST CENTER, SUITE 1900
1211 S.W. FIFTH AVE.
PORTLAND, OR 97204

EXAMINER	
TURCHEN, JAMES R	
ART UNIT	**PAPER NUMBER**
2139	

MAIL DATE	DELIVERY MODE
06/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/750,490	GOVINDARAJAN, PRIYA	
	Examiner	Art Unit	
	James Turchen	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 10-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8, 10-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-8 and 10-27 are pending. Claims 1, 2, 4-6, 10-12, 17, 19, 21, and 22 are amended. Claims 23-27 are new. Claim 9 is cancelled.

Response to Arguments

Applicant's arguments with respect to claims 1-8 and 10-27 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 6 and 10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 6 recites the limitation "the encrypted response packet" in first paragraph of claim 6. There is insufficient antecedent basis for this limitation in the claim.

Claim 10 recites the limitation "the method of claim 10" in the first line. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4, 7, 8, 10, and 23-27 are rejected under 35 U.S.C. 102(b) as being anticipated by Tyree (US 2002/0120853).

Regarding claims 1, 10, 25, and 26:

Tyree discloses identifying a DDoS attack identifier 330 identifying suspicious network activity (paragraph 70). Tyree discloses the countermeasure of DDoS attack as being located behind a first level of defense (paragraph 79) or at a firewall (paragraph 87, 88, and 89; the modules can be implemented on firewall 310). When implemented at the firewall 310, Tyree inherently discloses establishing a communication session between the firewall and the user device (by sending the question via HTML as seen in Figure 5., a TCP connection would need to be established between the firewall (monitor) and the user device). It is inherent to store the data access request while the authentication is underway. Tyree discloses sending a test to the first machine (paragraph 72). Additionally, Tyree discloses granting access to the originally requested service (paragraph 75). It is inherent to forward the request to the respective server via port forwarding. It is inherent for a firewall to use network address translation (NAT) to forward requests and responses to and from the respective server and by altering information in the header, the firewall effectively creates a "second session" (varying from the first session) that keeps outsiders from knowing the addresses of internal units. A "third session" is created by the combination of the first session and second session.

Regarding claims 2-4 and 27:

Tyree discloses FTP and HTTP (paragraph 47) that inherently uses the TCP/IP protocol for file connection. The first step of the three-way handshake of the TCP/IP protocol is the sending of a SYN from a first machine to a second machine. The second step of the three-way handshake is for the second machine to send a SYN-ACK to the first machine. The third step of the three-way handshake is for the first machine to send an ACK packet back to the second machine initiating the session between the two machines. TCP/IP additionally uses sequence numbers with each packet to ensure that data is delivered. The GET command is inherent in the HTTP protocol. The source and destination IP addresses are included in the TCP/IP header information.

Regarding claims 7 and 8:

Tyree discloses preparing a web page embodying the test (paragraph 72) and sending the web page to the first machine (paragraphs 85-91), and the test is embodied in a web page (figure 5).

Regarding claims 23 and 24:

Tyree discloses tracking by the monitoring device a number of attempts to establish communication sessions (paragraph 80, DDoS identifier detects an increase in server load which would be a result of an increased number of connections) and activating the defense system (paragraph 80). It is inherent that when there is no DDoS threat that the system operate as normal and that there will be no intelligence tests.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tyree as applied to claim 2 above, and further in view of Glawitsch (US 6,772,334) and Howard et al. (US 2003/0226034, herein Howard).

Regarding claim 5:

Tyree teaches all of the limitations of claim 2, but does not disclose generating a number to be included in the response packet by encrypting a first address on the network, a second address for the second machine, and a secret unknown to the first machine. Glawitsch discloses sending a SYN ACK packet with a pseudo acknowledgement number generated by taking the lowest 32-bits of a cryptographic checksum of the source address, destination address, source port number, destination port number, and sequence number of the IP header (column 7 lines 6-15) in order to facilitate validation of an ACK packet from the first machine responsive to the SYN ACK packet (column 9 lines 1-17). Glawitsch, however, does not disclose the inclusion of a secret unknown to the first machine in the number. Howard discloses including a key in the calculation of the number (paragraph 0036). It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Tyree to incorporate the cryptographic checksum in the SYN ACK packet in order to validate the session request (column 3 lines 1-4) and to include a key unknown to the first machine in order to allow the hashing algorithm to be known (paragraph 37).

Regarding claim 6:

Tyree, Glawitsch, and Howard disclose the method of claim 5, further including receiving the ACK packet from the first machine responsive to the response packet (Glawitsch, column 9 lines 1-17, client ACK packet 76 is received), decoding a tentative connection state information from the ACK packet (column 9 lines 7-10, the checksum is calculated using the same technique), and determining if the tentative connection state information is valid (column 9 lines 13-17).

Claims 11-22 correspond to the system and article of the method claims 1-8, 10, and 23-27 and are hereby rejected using the same reasoning.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

TAGHI ARANI
PRIMARY EXAMINER
6/22/10